UNITED STATES MARINE CORPS
COMMANDER, MARINE FORCES RESERVE
4400 DAUPHINE STREET
NEW ORLEANS, LOUISIANA 70146-5400

ForO 3300.1
3NBC
20 Jul 00

FORCE ORDER 3300.1

From: Commander, Marine Forces Reserve
To: Distribution List

Subj: MARINE FORCES RESERVE ANTITERRORISM/FORCE PROTECTION (AT/FP) PROGRAM

Ref: (a) DoD Dir 2000.12, Protection of DoD Personnel & Resources Against Terrorist Acts
(b) DoD Dir 2000.16, Combatting Terrorism Program Standards
(c) JSPUB 3-07.2, Joint Tactics, Techniques, and Procedures from Antiterrorism
(d) OPNAVINST 5530.14C, Navy Physical Security
(e) MCO 3302.1C, Marine Corps Antiterrorism/Force Protection Program
(f) MCO 3500.27, Operational Risk Management

Encl: (1) NCIS Foreign Counterintelligence POCs
(2) Bomb Threats
(3) Public Affairs Plan
(4) Terrorism/Law Enforcement/Security on the Internet
(5) Letter and Package Bomb Recognition Checklist
(6) Mission Essential Vulnerable Assets (MEVA)
(7) Area/Complex Physical Security Survey Tool
(8) CRAVER Target Analysis Tool
(9) Sample Vulnerability Assessment Format
(10) Formal Antiterrorism Training
(11) Travel Security Policy
(12) Terrorist Threat and Vulnerability Assessments
(13) Terrorist Threat Conditions (THREATCONS)
(14) Individual Protective Measures
(15) Physical Security Plan

1. Purpose. To establish policy, responsibilities, procedures and standards for the Marine Forces Reserve (MARFORRES) AT/FP Program at installations and bases in accordance with references (a) through (e). This Order contains information for U.S. Government use only and distribution is limited to U.S. Government agencies and personnel. Request for distribution of this document to outside personnel or agencies must be made to Commander, Marine Forces Reserve (COMMARFORRES) (ATTN: G-3).

2. Background

a. Terrorism, as defined in references (a) through (e), is the calculated use of violence or threat of violence to instill fear. Its purpose is to intimidate governments or societies in the pursuit of goals that are generally political, religious or ideological.

b. Terrorist acts have become more deadly and destructive. All Reserve forces must be prepared to defend themselves, their property and families in order to accomplish their missions.

c. The potential for terrorists to strike military personnel is documented throughout Marine Corps history. All Reserve personnel must possess the information needed to detect and defend against such acts.

d. The Department of Defense (DoD) describes force protection as a security program designed to protect military personnel, civilian employees, family members, facilities, and equipment in all locations and situations. This is accomplished through a planned and integrated application of antiterrorism, physical security program, operation security (OPSEC), personal protective services, and is supported by intelligence, counterintelligence, and other security programs. Antiterrorism can be defined as defensive measures, which reduce vulnerability to terrorist acts, and therefore is an integral part of the overall force protection concept.

e. The goal of the MARFORRES AT/FP program is to educate and train its Marines, Saliors, civilian employees and family members to protect themselves at home and abroad from acts of terrorism. Antiterrorism and Force Protection is a Commander's responsibility, however it is also an individual's responsibility to assist the Commander in protecting the personnel who comprise the Force by being vigilant and proactive in daily practice.

3. Information

a. The Department of Justice (DoJ) is the lead agency for combating domestic terrorism. Within the DoJ, the Federal Bureau of Investigation (FBI) is the lead agency for handling and investigating domestic terrorist acts committed in the United States.

b. The Department of State (DoS) is the lead agency for combating terrorism against American personnel and facilities outside the Continental United States (OCONUS). The DoS is also responsible for the foreign relations aspects of domestic

terrorism.

c. The Federal Aviation Administration (FAA) has exclusive responsibility for the direction of any law enforcement (if applicable) activity affecting the safety of persons aboard aircraft in flight involved in aircraft piracy. "In flight" is defined as that period when an aircraft's exterior doors are closed.

d. Federal law, inter-agency agreements, status-of-forces agreements (SOFAs), international agreements, and memorandums of understanding (MOUs) determine the DoD antiterrorism role. Military policies, directives, and plans support the DoJ and DoS under applicable federal laws or memorandums of agreement (MOAs). The DoD retains the command and control of all military forces involved in combating terrorist operations.

e. Enclosure (1) lists the ten field offices with NCIS Foreign Counterintelligence Agents, their areas of responsibility and the phone numbers for the counterintelligence POCs.

f. Enclosure (2) outlines basic procedures to follow when receiving a bomb threat and an example bomb threat checklist.

g. Enclosure (3) provides a basic AT/FP public affairs plan.

h. Enclosure (4) lists internet sites that provide unclassified AT/FP and travel guidance information.

i. Enclosure (5) is provided as a Letter and Package Bomb Recognition Checklist.

j. Enclosures (6) through (9) provide site vulnerability/target analysis tools. These tools are optional methods of determining installation vulnerability.

4. Policy

a. COMMARFORRES will protect military personnel and civilian employees, their families, government facilities, and material resources from acts of terrorism and other criminal and destructive acts. Commanding Officers will develop an operational capability that provides defense in depth against all threats. Commanding Officers will be guided by the provisions of this Order to be both proactive and reactive toward acts of terrorism and other criminal and hostile acts.

b. Commanders at all levels are required to integrate the standards of reference (a) into their AT/FP programs and shall develop subsequent prescriptive standards, based on the unit, installation, threat and operating environment, in order to satisfy unique AT/FP program requirements.

c. All commanders at the 185 individual MARFORRES sites spread throughout the country must clearly understand that assessment of terrorist/criminal threats to their site is inherently a local command responsibility. In short, identifying whether a site is threatened is a "bottom-up" process where the local commanders integrated NCIS reports and local police intelligence to assess the threat. Conversely when deploying outside the territorial limits of the United States the "top-down" threat assessment process is applicable, transmitted from the Theater CINCs via MARFORRES.

d. Force Protection (FP) encompasses more than essential AT procedures. It also incorporates the basic safety of our personnel. We will ensure their safety as a subset of FP using Operational Risk Management (ORM) techniques. ORM is a systematic decision-making process used to identify and manage hazards that could influence mission success and endanger assets. FP ORM will be incorporated in all levels of planning, scheduling and execution and will be addressed in all operations orders. Reference (f) provides detailed guidance on ORM.

e. FP will be incorporated/addressed in all Operation Orders issued within MARFORRES units.

5. Action. Marine Reserve Commanders/Commanding Officers/ Officers in Charge (Battalion/Squadron level and higher) will:

a. Appoint an AT/FP Officer in writing. This appointment may be an additional duty. The AT Officer assigned should be an Officer or SNCO, however exemption to the rank requirement will be granted for NCOs who are subject matter experts and have received formal training in AT/FP (i.e., military police, counterintelligence) as AT/FP Officers. Training requirements are identified in enclosure (10) of this order.

b. Ensure that units deploying OCONUS are assigned a Level II trained and certified AT/FP Officer. This individual shall serve as an advisor to assist the commander in meeting his AT/FP requirements. This individual shall, prior to deployment, ensure each person within the unit has received Level I training, is aware of the terrorism threat, and is trained to reduce risk or mitigate the effects should an attack occur.

c. Deliver a mandatory Level I brief and Area of Responsibility (AOR)/country specific threat information brief to all personnel planning to travel OCONUS regardless of threat level. Enclosure (11) can assist commands in explaining security measures to DoD personnel travelling abroad. In particular, close attention must be paid to the specific Theater CINC's AT/FP measures required of both individuals and units deploying to the specific CINC's AOR.

d. Develop comprehensive AT/FP programs that are based on current assessments of terrorist threats and unit vulnerabilities.

e. Establish Vulnerability and Threat Assessment programs. Commanders will request an assessment for their installation if their command is not aboard a major service base or installation. Vulnerability assessments will be requested via MARFORRES, AC/S G-3, AT/FP Officer (comm: 504-678-8086/1284). Enclosure (11) provides detailed instructions on scheduling and conducting threat and vulnerability assessments.

f. Establish command AT/FP information and awareness programs to ensure all assigned personnel to include Marines, sailors, family members and civilian employees are aware of the general terrorist threat and the personal protection measures that could reduce individual vulnerability to acts of terrorism. Additionally, command information programs shall be capable of ensuring that all personnel are informed of increased threat condition (THREATCON) levels and the measures to be taken and implemented. Enclosure (13) provides specific information on threat conditions.

g. Develop a means of mass notification of unit and installation personnel via recognizable alarms for potential emergencies. These alarms should possess a capability to immediately sound the alarm, should have their own set of reactions, and should be drilled frequently to familiarize all personnel with individual responsibilities.

h. Ensure that country and theater clearances are requested for each foreign country prior to units or individual travelling OCONUS.

i. Provide initial threat and security briefings to all newly assigned military, civilian personnel and their dependents when a unit is located overseas. Enclosure (14) provides fundamental individual protective measures.

j. Provide guidance annually to all personnel assigned to medium and high threat locations on appropriate conduct in the event they are taken hostage or kidnapped.

k. Provide information on vehicle bomb searches to all personnel and include a copy on all government trip tickets.

l. Ensure that personnel in receipt of orders OCONUS receive the Level I threat brief and AOR Specific threat brief for themselves and their dependents. Certification of the training must be included in the serviceman's record and on orders. This requirement is the "losing Commanders'" responsibility. Develop prescriptive AT/FP standards based on the type of unit, installation location, potential threat and operating environment.

m. Develop and implement security procedures to defend against terrorism, and support these procedures with adequate planning and evaluation. For independent activities this may include the revision of existing local security directives and physical security equipment. Enclosure (15) provides more detailed guidance on physical security plans.

n. Ensure plans, procedures, assessments, and training address potential threats to information systems and the potential use of Weapons of Mass Destruction (WMD). Programs shall include plans and procedures for crisis/consequence management, first responder, and medical response.

o. Conduct an annual AT/FP exercise at their installation. This exercise will be concurrent with real-time terrorist threats.

p. Develop AT/FP plans that include a process, based on terrorism threat information and/or guidance from higher headquarters, to raise or lower THREATCON levels. Subordinate Commanders may raise but not lower a higher level Commander's THREATCON. Plans will also address procedures to collect and analyze threat information and threat capability, assess vulnerability to threat attacks, implement procedures to enhance AT/FP, and procedures for responding to threat incidents. AT/FP plans will also be reviewed and updated annually.

q. The Naval Criminal Investigative Service (NCIS) maintains a world-wide structure which provides counterintelligence and anti-terrorism support to Marine Corps commands. Within the United States there are ten special agents serving ten geographical areas as an available source for such information. Enclosure (1) lists the ten field offices with NCIS Foreign Counterintelligence Agents, their areas of responsibility and the phone numbers for the counter-intelligence POCs. Commanders will insure unit AT/FP Officers and Security Managers contact the nearest field office to obtain access to local threat information.

r. State, county, and city law enforcement agencies receive information concerning local threats from their own intelligence sources. This information may be provided to local Marine Corps sites if liaison with the law enforcement agency is maintained. Commanders will insure unit AT/FP Officers and Security Managers contact state, county and city law enforcement agencies obtain access to local threat information.

6. Recommendations for Changes. Submit recommendations for changes to this order via the chain of command to this headquarters (attn: G-3/AT/FP).

7. Reserve Applicability. This Order is applicable to the Marine Corps Reserve.

P. J. DULIN
Chief of Staff

DISTRIBUTION: A

ForO 3300.1
20 Jul 00

NCIS FOREIGN COUNTERINTELLIGENCE POCs

PENSACOLA FIELD OFFICE
(850) 452-3835 DSN 922-3835
AL
AR
FL (Tallahassee & West)
IL
IN
KS
KY
LA
MI
MN
MS
MO
NE
ND
IA
OK
SD
TN
WI

PEARL HARBOR FIELD OFFICE
(808) 474-1218 DSN: 315 474-1218
HI

LOS ANGELES FIELD OFFICE
(909) 985-2264933-5611
So CAL Counties of
LA, Co
Orange, Co
Ventura
Santa Barbara
San Luis Obispo
Riverside
San Bernadino
Mono
Inyo
All No CAL
NV Co (Clark
& Las Vegas)
CO
UT
WY

SAN DIEGO FIELD OFFICE
(619) 556-1364 DSN: 526-1364
SD Co, CA
AZ
TX Counties (El Paso, Hudspeth, Reeves, Culberston)
Imperial Co, CA
NM

MAYPORT FIELD OFFICE
(904) 270-5361 DSN: 960-5361
GA
Florida (East & South of Tallahassee)

NEWPORT FIELD OFFICE
(401) 841-2241 DSN: 948-2241
CT
MA
ME
NH
NJ
NJ
PA
RI
VT

LEJEUNE FIELD OFFICER
II MEF: (910) 451-8009 DSN: 751-8009
NC Counties of:
Brunswick
Columbus
Cumberland
Duplain
EdgeComb
Hoke
Jones
Lenor
New Hanover
Onslow
Pinder
Roberson
Sampson
Wayne

NORFOLK FIELD OFFICE
(757) 444-7327 DSN: 564-7327
SE VA Counties EXCEPT:
Orange
Green
Madison
Rockingham
Shenandoah
Rappahannock
Warren
Clarke
Frederick
Page

WASH D.C. FIELD OFFICE
(202) 433-3858 DSN: 288-3858
MD
D.C.
D.E.
WV
VA Counties of:
Aacomack
Arlington
Caroline
Clarke
Culpeper
Essex
Fairfax
Fauquier
Frederick
Green
George
Lancaster
Loudon
Madison
N. Hampton
Orange
Page
Prince William
Rappahannock
Rockingham
Shenandoah
Spotsylvania
Stafford
Warren
Westmoreland
Warren
VA Cities of:
Falls Church
Fairfax King
Vienna
Fredericksburg

PUGET SOUND FIELD OFFICE
(306) 396-4660 DSN: 744-4660
AK
WA
OR
ID
MT

ENCLOSURE (1)

BOMB THREATS

1. General. Bombs and Improvised Explosive Devices (IEDs) are ideal tools that terrorists use to demonstrate ineffectiveness of government services. They are low cost, allow for escape of the perpetrator, and easily create the chaos, intimidation and coercion that the terrorist seeks.

2. Actions. It is imperative that personnel involved in a search or in normal routine work activity be instructed that their only mission is to locate and report suspicious objects. Under no circumstances should anyone move, jar, or touch an unconfirmed explosive object or anything attached to it. The removal or disarming of a bomb must be left to the professionals in explosive ordnance disposal. Rules to be followed upon identification of a bomb or suspected bomb:

a. Report the location and an accurate description of the object to the appropriate person. This information will be relayed immediately. Emergency response personnel should be met.

b. If possible and so equipped, take several pictures of the device. Do not use flash bulb attachments or flash settings on the camera.

c. Move as far away from the suspect object as possible without being placed in further danger from other hazards (traffic, secondary explosives, flammables, etc.). Identify the danger area, and block it off with a clear zone of at least 300 feet, including floors above and below the object.

d. Keep away from glass windows or other materials that can become additional flying debris Stay out of "line of sight" of the object, thereby reducing hazard of injury as a consequence of direct fragmentation. If absolutely necessary, place sandbags or mattresses, never metal shields, around the suspicious object. Do not attempt to cover the object. If possible, check to see that all doors and windows are open to minimize primary damage from the blast and secondary damage from fragmentation.

d. Remain alert for additional or secondary explosive devices in the immediate area, especially if location of the bomb evacuation-assembly area is widely known.

3. Immediate Action. Immediate action may include search without evacuation, movement of personnel within the establishment, partial evacuation, or total evacuation. If evacuated, do not permit re-entry into the building until the device has been rendered safe and removed, and the building declared safe for re-entry. Analysis and evacuation criteria will be a matter of local SOP. It must be command directed, instructed and exercised.

4. Telephone Bomb Threats. Telephonic threats can achieve the desired disruption with little risk or effort on part of the terrorist. Treat all calls seriously, although subsequent search reveals them to be hoax. Upon receiving an anonymous telephone call, try to:

a. Write down conversation (see page 3 of this enclosure).

b. Obtain the caller's name, address, and telephone number. Point out to the caller that by giving these details, he or she is indicating that the call is a genuine warning.

c. Keep the caller talking and elicit as much information as possible.

d. Summon assistance (through a telephone exchange) to trace the call and corroborate facts and opinions.

e. Comply with the caller's request to be connected with another extension. Monitor the call if possible. Alert the security officer or the command duty officer IMMEDIATELY.

TELEPHONE BOMB THREAT

1. BOMB THREAT RECEIVED ON PHONE NUMBER: _____

2. BOMB THREAT RECEIVED AT: _____

3. **KEEP CALLER ON THE LINE!**

4. NOTIFY THE PHONE COMPANY (PHONE NUMBER ___-____) OF THE THREAT AND REQUEST IMMEDIATE LINE TRACE.

5. CALLER STATES THE BOMB IS LOCATED AT:

_____

_____

_____

_____

6. THE CALLER SAYS THE BOMB WILL EXPLODE:

(WHEN) _____

7. THE CALLER HAS MADE THE FOLLOWING THREATS/DEMANDS:

_____

_____

_____

_____

_____

8. OTHER COMMENTS:

_____

_____

_____

ENCLOSURE (2)

ForO 3300.1
20 Jul 00

PUBLIC AFFAIRS PLAN

1. Public Affairs Audiences. Public Affairs actions regarding antiterrorism/force protection should be focused toward two audiences:

a. Internal (Marines, Sailors and family members).

b. External (general public).

2. Internal Audiences. Information regarding the entire AT/FP Program should be regularly provided to and discussed with your internal audiences. Various aspects of the program could be included in unit newsletters to keep people aware of the potential for terrorism and how to combat it. As threat conditions change, your internal audiences will be reminded of the requirements of the new threat condition. Education and awareness will help ensure that the internal audiences are prepared for any potential or real terrorist activity.

3. External Audiences. External audiences such as the media and the general public may, at times, be very interested in what a military unit is doing with regards to antiterrorism/force protection. Their interest will become especially evident if a threat condition changes, as they will notice a change in unit activities. It is important to respond to their questions; however, security precautions should not be specifically discussed, as that could jeopardize a unit's security. General statements such as, "We are reviewing our security procedures and ensuring appropriate measures are in effect to adequately safeguard our personnel and property," can be used. MARFORRES Public Affairs should be informed about specific media queries in this regard. The public affairs office is also available to assist with formulating responses to media queries. Phone numbers for the MARFORRES Public Affairs Office are (504) 678-1227/4117.

ENCLOSURE (3)

ForO 3300.1
20 Jul 00

TERRORISM/LAW ENFORCEMENT/SECURITY INFORMATION ON THE INTERNET

1. Government Addresses

U.S. Department of State, Consular Affairs:
http://travel.state.gov

U.S. Department of State: http://www.heroes.net/

Counterterrorism: http://state.gov/www/global/terrorism/
index.html

Federal Bureau of Investigation Homepage: http://www.fbi.gov/

Central Intelligence Agency: http://www.odci.gov/cia/

2. Terrorism Related Addresses

J34 Homepage on GCCS: http://nmcc20a/-d@c@e@-ap/j34.htm/

Department of Defense Antiterrorism Homepage:
www.dtic.mil/jcs/force_protection/

Terrorism Research Center:
www.terrorism.com/terrorism/index.html

Report to the President and Congress on the Protection of U.S.
Forces Deployed Abroad:
http://www.dtic.mil/defenselink/pubs/downing-rpt/

Hot Topics-Terrorism/Antiterrorism: http://www.dtic.mil/

Terrorism: http://www.upapubs.com/
Center for the Study of Terrorism and Political Violence:
http://www.st-and.ac.uk/-www-shir/terr.html

Rand Homepage: http://www.rand.org/

Kroll Associates: http://www.Krollassociates.com/

Stormfront White Nationalist Resource Page:
http://www.stormfront.org/

HateWatch Guide to Hate Groups on the Internet:
http://hatewatch.org/

ENCLOSURE (4)

Profiles Threat Counter Measures Group:
http://www.profiles--tag.com/

Terrorism and Political Violence Home Page:
http://www.frankcas-s.com/jnis/tpv.htm

The Counter-Terrorism Page: http://www.terrorism.com/

Counter Terrorism Homepage:
http://www.worldonline.net/securitynet/CTS/index.html

Federal Emergency Management Administration's Fact Sheet on Terrorism: http://www.fema.gov/fema/terrorf.html

Israel INTERNET Terrorism Hotline: http:/shani.net/terror/

Library of Congress Search Engine: Terrorism:
http://Icweb.loc.gov/lexico/tgml/t/Terrorism.html

Internet: Terrorism: http://www.milnet.com/milnet/terror.htm

Society and Culture: Crimes: Terrorism:
http://www.yahoo.com/Society-and-Culture/Crime/Crimes/Terrorism/

Terrorist Profiles:
http://nsi.org/Library/Terrorism/profterr.txt

Terrorist Use of Chemical Weapons:
http://groucho.la.asu.edu/-jvim/IntelligenceBriefing

MCI link:
www.mci.hqi.usmc.mil/support-files/mci-news/terrorism/main.htm

CD-i's Counter-Terrorism issues page:
http://www.cdt.org/policy/terrorism/

International Policy Institute for Counter-Terrorism:
http://www.ict-org.il/

3. AOR Specific/Country Specific Addresses

PACOM Homepage: www.pacom.mil/direct/at/athome.htm

EUCOM Homepage: www.eucom.mil

ENCLOSURE (4)

CENTCOM Homepage: www.centcom.mil

SOUTHCOM Homepage: www.ussouthcom/southcom/

USACOM Homepage: 137.246.33.240:8000/acomweb.nsf

Department of State, Travel Threat Advisories:
http://travel.state.gov/travel-warnings.html

Ariga: The Pinkerton Daily Risk Assessment for the Middle East:
http://ariga.co.il/pink.htm

4. Security/Law Enforcement Addresses

Provost Marshal/Intelligence link:
www-ioc.army.mil/dm/DMPWEB/links.htm

U.S. Army MP school: www.mcclellan.army.mil/usamps/dots/aletd

NCIS Homepage: www.ncis.navy.mil

Air Force Security Forces Home Page:
http://www.kirtland.af.mil/organizations/AFSF/

American Society for Industrial Security:
http://www.asisonline.org/
Security Management Online: http://www.securitymanagement.com/

International Association of Chiefs of Police:
http://www.amdahl.com/ext/iacp/

Cecil Greeks's Criminal Justice Page:
http://www.stpt.usf.edu/-greek/cj

Office of International Criminal Justice:
http://www.acsp.uic.edu/

National Industrial Security Board:
http://www.dis.mil/page20.htm

Corporate Security Resources Page:
http://chelsea.ios.com/-glenz/

Pinkerton Risk Assessments: http://www.ipn.net/pinkerton.htmi

Law enforcement (if applicable) Product News:
http://www.law-enforcement.com/

Justice Information Technology Network: http://www.nlectc.org/

Security Groups and Organizations:
http://www.alw.nih.gov/security/security-groups.html

NASA Security Homepage:
http://nasirc.nasa.gov/rthomas/homepg.html

Scotti School WWW Homepage: http://www.ssdd.com/sscschd97.html

Code 7 Cafe, Firearms Information:
http://www.av.qnet.com/-harv/index.htm

5. Publications Addresses

Department of Defense Publications: web7.whs.osd.mil/corres.htm

Joint Staff Publications: www.dtic.mil/jcs/people.html

Navy Directives: www.dodssp.daps.mil/usndirs.htm

USMC doctrine: 138.156.107.3/docdiv/

FBI publication: Terrorism in the United States:
www.fbi.gov/publish/terror/terrusa.htm

DOS publication: Patterns of Global Terrorism:
www.state.gov/global/terrorism/1997Report/1997index.html

6. Programs and Resources

Physical Security Equipment Action Group: www.csc.com/pseag

Force Protection Equipment Demonstration: www.csc.com/fped

MARCORSYSCOM homepage: www.marcorsyscom.usmc.mil

7. Other Related Links

Federal Web Locator: www.law.vill.edu/fed-agency/fedwebloc.html

U.S. Military Internet sites: www.dtic.mil/

ENCLOSURE (4)

Joint Lessons Learned:
www.jwfc.js.mil/pages/jcllbull/antiter.htm

Congressional Action: http://thomas.loc.gov/

Marine Corps Homepage: www.usmc.mil

Navy Homepage: www.navy.mil

Airforce Homepage: www.af.mil

Army Homepage: www.army.mil

Army National Guard, Weapons of Mass Destruction:
www.ngb.dtic.mil

Marine Corps Concepts Division:
http://138.156.107.3/concepts/home.html

Chemical Biological Incident Response Force (CBIRF.) Homepage:
www.cbirf.usmc.mil

ForO 3300.1
20 Jul 00

Letter And Package Bomb Recognition Checklist

The following information is useful in detecting the presence of letter or package bombs sent through US and international mails. Letters and packages exhibiting the characteristics below should be considered as potential Improvised Explosive Devices (IEDs).

WEIGHT
--------- weight unevenly distributed
--------- heavier than usual for its size
--------- heavier than usual for its postal class
STAMPS
--------- more than enough postage
POSTMARK
--------- foreign from an unusual city
THICKNESS
--------- for medium size envelopes, the thickness of a small book
--------- not uniform or has bulges
--------- for large envelopes, bulkiness, an inch or more
WRITING
--------- foreign writing style
--------- misspelled words
--------- marked "air mail," "registered," "certified," or "special delivery certified," or "special delivery"
ADDRESS
--------- marked "personal," "private," or "eyes only confidential"
--------- no return address
--------- poorly typed or handwritten address
--------- hand printed
--------- title for the recipient incorrect
--------- addressed to a high-ranking recipient by name or title
ENVELOPE
--------- peculiar odor
--------- oil stains
--------- inner sealed enclosure
--------- excessive sealing material
--------- wire, string, or foil sticking out of package
--------- ink stains
RIGIDITTY
--------- springiness
--------- greater than normal, particularly along its center length

ENCLOSURE (5)

MISSION ESSENTIAL VULNERABLE ASSETS (MEVA)

1. General. This enclosure identifies some potential MEVAs, and provides one manner a commander may use to preliminarily identify MEVAs at the installation. It's use is not required.

2. MEVA. The commander bears responsibility for determining the criticality of the site/installation's assets to successfully accomplish its mission, even if the threat inflicts casualties and destroys or damages assets. MEVA may include:

a. command headquarters

b. computer center

c. arms room

d. communications center

e. motor pool

f. aviation complex

g. any item(s) that will have an impact on the site/installation commander's mission.

3. Security Priorities. By combining physical security system components into an integrated protection system (a "system of systems"), it is possible to achieve appropriate levels of protection for installation defense. Such systems can be prohibitively expensive if applied to each of the installation's facilities. Since resources are seldom unlimited, the Commander must establish physical security protection priorities based upon the MEVA. The levels of priorities of protection include:

a. Level A: Assets, the loss, theft, destruction, or misuse of which will result in great harm to the strategic capability.

b. Level B: Assets, the loss, theft, destruction, or misuse of which will result in grave harm the operational capabilities.

c. Level C: Assets, the loss, theft, destruction, or misuse of which could impact upon the tactical capabilities.

d. Level D: Assets, the loss, theft destruction or misuse of which could compromise the defense infrastructure.

4. Sensitive Equipment. The commander should use all of the physical security expertise available. This expertise complements the technical knowledge in other staff areas. Sensitive equipment and/or complexes may require differing degrees and types of protection depending on the physical characteristics of each location, surrounding environment, and vulnerability to security hazards.

7. Medical.

a. Location

b. Size

c. Capacities

d. Security and date of last rehearsal

e. Reaction time to mass trauma and last rehearsal

f. Special assets (helicopter pad, vehicles, airfields, medical treatment)

8. Communications/Power Systems.

a. Main terminals/substations

b. Layout of complete grid system (electrical and phone)

c. Grid system central points/communications control points

d. Special capabilities (tract, tap, isolate)

9. Municipal Emergency Plans.

a. Function of each organization

b. Location of crisis action command post

c. Chain of command

d. Last rehearsal of emergency plans

10. Photos.

a. Aerial (N,S,E,W, and direct overhead)

b. Ground photo facing out to surrounding area

c. Ground photo facing into facility

d. Determine location of "unfriendly" government buildings, commercial/social action/political organization, and areas of known unrest

11. History of activity as it effects the current government (if OCONUS).

12. Potential of negative activity against current government (if OCONUS).

13. List of all agencies, officials, and government with any degree of responsibility and authority.

14. List of any commercial corporations or private citizens who have significant "power behind the throne" influence.

15. Identify staging areas for emergency reaction teams.

CARVER Target Analysis Tool

1. General. The following is an explanation of the CARVER targeting process. This process is used by US Special Operations Forces (SOF) in targeting adversary's installations. For that reason it is included as a tool to evaluate US installations from an adversarial point of view. Its use is not required.

2. Target Analysis Process. This enclosure explains CARVER, which is a SOF term. CARVER is used by Army Special Operations (ARSOF) personnel, Security Information Officers, and operational personnel throughout the ARSOF targeting and mission planning process to assess mission, validity, and requirements. It is also used in technical appreciation and target analysis. This enclosure provides a step-by-step example of how to use CARVER.

3. Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability Factors. The CARVER selection factors assist in selecting the best targets or components to attack. As the factors are considered, they are given a numerical value. This value represents the desirability of attacking the target. The values are then placed in a decision matrix. After CARVER values for each target or component are assigned, the sum of the values indicate the highest value target or component to be attacked within the limits of the statement of requirements and commander's intent.

a. Criticality. Criticality means target value. This is the primary consideration in targeting. A target is critical when its destruction or damage has a significant impact on military, political, or economic operations. Targets within a system must be considered in relation to other elements of the target system. The value of a target will change as the situation develops, requiring the use of time-sensitive methods to respond to changing situations. For example, when one has few locomotives, railroad bridging may be less critical as targets; however, safeguarding bridges may be critical to maneuvering conventional forces that require use of such bridges. Criticality depends on several factors:

(1) Time: How rapidly will the impact of the target attack affect operations?

ENCLOSURE (8)

(2) Quality: What percentage of output, production or service will be curtailed by target damage?

(3) Surrogates: What will be the effect on the output, production, and service?

(4) Relativity: How many targets are there? What are their positions? How is their relative value determined? What will be effected in the system or complex "stream"? Table 1 shows how criticality values are assigned on CARVER matrixes.

Table 1. Assigning Criticality Values.

CRITERA	SCALE
Immediate halt in output, production or service; target cannot function without it	9-10
Halt within 1 day, or 66% curtailment in output, production or services	7-8
Halt within 1 week, or 33% curtailment in output, production, or services	5-6
Halt within 10 days, or 10% curtailment in output, production or services	3-4
No significant effect	1-2

b. Accessibility

(1) A target is accessible when an operational element can reach the target with sufficient personnel and equipment to accomplish its mission. A target can be accessible even if it requires the assistance of knowledgeable insiders. This assessment entails identifying and studying critical paths that the operational element must take to achieve its objectives, and measuring those things that aid or impede access. The adversary must not only be able to reach the target but must also remain there for an extended period. The four basic steps identifying accessibility are:

(a) Infiltration from the staging base to the target area.

(b) Movement from the point of entry to the target or objective.

(c) Movement to the target's critical element.

(d) Exfiltration.

(2) Factors considered when evaluating accessibility include, but are not limited to:

(a) Active and passive early warning systems.

(b) Swimmer detection devices.

(c) Air defense capabilities within the target area.

(d) Road and rail transportation systems.

(e) Type of terrain and its use.

(f) Concealment and cover.

(g) Population density.

(h) Other natural or synthetic obstacles/barriers.

(i) Current and climatic weather conditions.

(3) The analysis along each critical path to the target should measure the time it would take for the action element to bypass, neutralize, or penetrate barriers and obstacles along the way.

(4) Accessibility is measured in terms of relative ease or difficulty of movement for the operational element and the likelihood of detection. The use of standoff weapons should always be considered in such evaluations.

Table 2. Assigning Accessibility Values.

CRITERA	SCALE
Easily accessible, standoff weapons can be employed	9-10
Inside a perimeter fence but outdoors	7-8
Inside a building but on ground floor	5-6
Inside a building but on second floor or in basement; climbing or lowering required	3-4
Not accessible or inacessible without extreme difficulty	1-2

c. Recuperability. A target's recuperability is measured in time; that is, how long will it take to replace, repair, or bypass the destruction of, or damage to the target? Recuperability varies with the sources and type of targeted components and the availability of spare parts. Factors which should be considered when assessing recuperability include, but are not limited to, the availability of:

(1) On-hand equipment such as railroad cranes, dry docks, and cannibalization.

(2) Restoration and substitution through redundancies. On hand spares.

(3) Equivalent equipment sets that backup critical equipment or components, and the effects of economic embargoes and labor unrest.

Table 3. Assigning Recuperability Values.

CRITERIA	SCALE
Replacement, repair or substitution requires 1 month or more	9-10
Replacement, repair or substitution requires 1 week to 1 month	7-8
Replacement, repair or substitution requires 72 hours to 1 week	5-6
Replacement, repair or substitution requires 24 to 72 hours	3-4
Same day replacement, repair or substitution	1-2

d. Vulnerability.

(1) A target is vulnerable if the adversary has the means and expertise to successfully attack the target. When determining the vulnerability of a target, the scale of the critical component needs to be compared with the capability of the attacking element to destroy or damage it. In general, the attacking element may tend to:

(a) Choose special components.

(b) Do permanent damage.

(c) Prevent or inhibit cannibalization.

(d) Maximize effects through the use of onsite materials.

(e) Cause the target to self-destruct.

(2) Specifically, vulnerability depends on:

(a) The nature and construction of the target.

(b) The amount of damage required.

(c) The assets available; for example, personnel, expertise, motivation, weapons, explosives, and equipment. Table 4 shows how vulnerability values are assigned on CARVER matrices.

Table 4. Assigning vulnerability values.

CRITERIA	SCALE
Vulnerable to long-range laser target designation, small arms fire or charges of 5 pounds or less	9-10
Vulnerable to light anti-armor weapons fire or charges of 5 to 10 pounds	7-8
Vulnerable to medium anti-armor weapons fire, bulk charges of 10 to 30 pounds or very careful placement of smaller charges	5-6
Vulnerable to heavy anti-armor fire, bulk charges of 30 to 50 pounds or requires special weapons	3-4
Invulnerable to all but the most extreme targeting measures	1-2

e. EFFECT. The effect of a target attack is a measure of possible military, political, economic, psychological, and sociological impacts at the target and beyond. This is closely related to the measure of target criticality. The type and magnitude of given effects desired will help the adversary select targets and target components for attack. Effect in this context addresses all significant effects, whether desired or not, that may result once the selected target component is attacked. Traditionally, this element has addressed the effect on the local population, but now there are broader considerations. Effect is frequently neutral at the tactical adversarial level. For example, the primary effect of the destruction of two adjacent long-range radar sites in an early warning system may be to open a hole in the system that is of sufficient size and duration to permit our adversary to launch a successful attack against the installation. Effects can also include:

(1) The triggering of countermeasures.

(2) Support or negation of PSYOP themes.

(3) Unemployment.

(4) Reprisals against the civilian populace.

(5) Collateral damage to other targets.

Table 5. Assigning effect values.

CRITERIA	SCALE
Overwhelmingly positive effects; no significant negative effects	9-10
Moderately positive effects; no significant negative effects	7-8
No significant effects, neutral	5-6
Moderately negative effects; few significant positive effects	3-4
Overwhelmingly negative effects; no significant positive effects	1-2

f. Recognizability. A target's recognizability is the degree to which it can be recognized by the adversary and his intelligence collection and reconnaissance assets, under varying conditions. Weather has an obvious and significant impact on visibility. Rain, snow, and ground fog may obscure observation. Road segments with sparse vegetation and adjacent high ground provide excellent conditions for good observation. Distance, light, and season must also be considered. Other factors that influence recognizability include the size and complexity of the target, the existence of distinctive target signatures, the presence of masking or camouflage, and the technical sophistication and training of the adversary.

Table 6. Assigning recognizability values.

CRITERIA	SCALE
The target is clearly recognizable under all conditions and from a distance; it requires little or not training for recognition	9-10
The target is easily recognizable at small-arms range and requires a small amount of training for recognition	7-8
The target is diffcult to recognize at night or in bad weather, or might be confused with other targets or target components; it requires some training for recognition	5-6
The target is difficult to recognize at night or in bad weather, even within small-arms range; it is easily confused with other targets or components, it requires extensive training for recognition	3-4
The target cannot be recognized under any conditions, except by experts	1-2

4. Carver Matrix

a. These CARVER factors and their assigned values are used to construct a CARVER matrix. For the adversary this is a tool for rating the desirability of potential targets and wisely allocating attack resources. For the installation commander, it is a tool to counter the adversary.

b. To construct the matrix, list the adversary's potential targets in the left column. For strategic level analysis, list the installation's systems or subsystems (electric power supply rail system). For tactical level analysis, list the complexes o components of the subsystems or complexes selected by your Mission Essential Vulnerable Asset (MEVA) analysis. (Figure 1 shows a sample matrix for a bulk electric power supply facility

c. As each potential target is evaluated for each CARVER factor, enter the appropriate targets that have been evaluated, add the values for each potential target. The sums represent th relative desirability of each potential target; this constitute a prioritized list of targets. Attack those targets with the highest totals first.

d. If additional men and/or munitions are available, allocate these resources to the remaining potential targets in descending numerical order. This allocation scheme will maximiz the use of limited resources. Planners can use the CARVER matri to present the installation's staff with a variety of adversary defeat options. With the matrix they can discuss the strengths and weaknesses of each COA against the installation's targeted facility.

POTENTIAL TARGETS	C	A	R	V	E	R	TOTAL
Fuel tanks	8	9	3	8	5	6	41
Fuel pumps	8	6	2	10	5	3	34
Boilers	6	2	10	4	5	4	31
Turbines	8	6	10	7	5	9	45

SAMPLE VULNERABILITY ASSESSMENT FORMAT

1. This enclosure contains a sample format that can be used to perform vulnerablitilty assessments. The purpose of a vulnerability assessment is to aid commanders in identifying the following:

a. Weaknesses in physical security plans, programs and structures.

b. inefficiencies and diminishing effectiveness in personnel practices and procedures relating to security, incident control, incident response and incident resolution including, but not limited to, law enforcement and security, intelligence, command, communications, medical and public affairs.

c. Enhancements in operational procedures during times of peace, mobilization, crisis and war.

d. Resource requirements necessary to meet DoD, Service and local security requirements.

2. Vulnerability assessments are continuous, based on the operational tempo and local threat level. Commanders may also use vulnerability assessments for other management, training and oversight purposes.

ForO 3300.1
20 Jul 00

VULNERABILITY ASSESSMENT FORMAT

Classification

letter head/address

FORCE PROTECTION VULNERABILITY ASSESSMENT

Reported By: File Number:
Period of Report: Date of Report:

Matters Investigated: Force Protection Vulnerability Assessment of _____.

Status: (Open/Closed/Referred for Information)

signature

Distribution:

Special Handling Required: (if applicable)

Property of:

Classified By:
Reason:
Declassify On:

Classification

ENCLOSURE (9)

1. EXECUTIVE SUMMARY:

- Reason for assessment; i.e. annual, command directed.

2. MISSION STATEMENT:

- Installation/facility/unit mission/purpose.

3. ASSIGNED THREAT LEVEL:

- Current assigned threat level.

4. THREAT ASSESSMENT:

a. Terrorist Threat:

- Is there state sponsored terrorism?
- Is there a transitional terrorist threat?
- Are there indigenous terrorist/dissident groups in area?

b. Third Country National:

- Is there a non-indigenous personnel threat? (for OCONUS)

c. Foreign Intelligence Service Threat:

- What is the host-country intelligence threat? (for OCONUS)
- What is the threat country intelligence threat?
- Is there an intelligence threat posed by members of a coalition/allied forces?

d. Criminal Threat:

- What is the local history of criminal activity?
- What is the status of local gang activity?

5. GENERAL GEOGRAPHIC AND DEMOGRAPHIC SETTING:

a. Installation/Facility Location:

- Where is the installation/facility?
- What are the basic topographic features in and around the installation?

- What are the basic sociological and demographic conditions around the installation?

b. Access to Target Area:

- What are the land routes into the installation?
- What are the underground routes into the installation?
- Is the installation accessible by air?

6. EXTERNAL SECURITY:

a. Law Enforcement and Security Environment:

- Which governmental departments, agencies and organizations have law enforcement responsibilities, investigative responsibilities and prosecutorial responsibilities external to the installation.
- Which state/local departments, agencies and organizations have law enforcement responsibilities, investigative responsibilities and prosecutorial responsibilities external to the installation.
- Is there a history of security problems or law enforcement problems in and around the installation?

b. Perimeter Security and Entry Control:

- What types of barriers, penetrations, penetration surveillance and control systems, locks intrusion detection systems, and security lighting systems are used?
- Who is responsible for selection, operation, maintenance, and replacement of each perimeter security component?

c. Security Personnel and Perimeter Guards:

- Who mans perimeter penetration control systems? What are their specific duties and responsibilities? Who is responsible for oversight, training and discipline of the guard force?
- Are gate guards and security personnel armed? If so, have they been trained? To what standards? How often? Assessed and certified by whom? Is Deadly Force authorized? Have personnel been trained in the use of Deadly Force?

7. Internal Security:

a. Law Enforcement and Security Environment:

- Which governmental departments, agencies and organizations have law enforcement responsibilities, investigative responsibilities and prosecutorial responsibilities on the installation.
- Is there a history of security problems or law enforcement problems in and around the installation?

b. Perimeter Security and Entry Control:

- What types of barriers, penetrations, penetration surveillance and control systems, locks intrusion detection systems, and security lighting systems are used?
- Who is responsible for selection, operation, maintenance, and replacement of each perimeter security component?

c. Security Personnel and Perimeter Guards:

- Who mans perimeter penetration control systems? What are their specific duties and responsibilities? Who is responsible for oversight, training and discipline of the guard force?
- Are gate guards and security personnel armed? If so, have they been trained? To what standards? How often? Assessed and certified by whom? Is Deadly Force authorized? Have personnel been trained in the use of Deadly Force?

8. INTERIOR OF BUILDINGS AND FACILITIES:

- What materials were used in construction of buildings exterior and interior work spaces? What was the method of construction? Do plans for each structure or significant working area within each structure exist?
- How many penetrations between the exterior and interior exist? How are windows, doors and utility connection penetrations constructed? How is access to the interior of the building monitored and controlled?
- Are there any obscure building exterior penetrations such as side walk elevators, storm sewers or utility tunnels? Are there any tunnels, conduits, pedestrian or vehicle passages which run under the building, but do not afford access to the interior of the building?

9. FACILITY/OFFICE OPERATIONS AND ACCESS CONTROL:

- Describe normal facility operations in terms of work hours, employee identification, access control procedures in use, ect.
- Where do vehicles park? How is access to parking facilities controlled?
- How are keys to the facility and secure areas within the facility controlled?
- How are mail and other small package shipments processed into and out of the installation/faciltiy?
- How is the installation/facility alarmed to warn personnel of natural disaster, fire, bomb threat or other emergency?

10. CONTRACTOR, VENDOR AND VISITOR CONTROL:

- How are contractors, vendors and other visitors identified, granted access and controlled once they enter the installation or facility?
- What measures are followed to ensure the security of facilities after all contractors, vendors and other visitors have departed?

11. LOGISTIC SUPPORT:

a. Rations:

- Are the rations stored in a secure location? Transported or locally procured? By whom? Are emergency rations available?

b. Water:

- Potable/non-potable?
- What is the storage location? Underground or above ground? Transported or locally procured? Are emergency rations available?

c. Utilities:

- What is the installation/facility power source?
- What is the security protection provided for the main and emergency power source?

d. Communications:

- Identify primary, alternate, secure and non-secure communications available.

e. Emergency Services:

- Is police, fire, hospital support available?
- What is each response time?
- How are they contacted?

12. OTHER OBERVATIONS AND RECOMMENDATIONS:

- Unique mission requirements.
- Waivers and exceptions.
- Unusual observations or repeat observations.

13. EXHIBITS:

- Maps, photographs, diagrams, etc.

FORMAL ANTITERRORISM TRAINING

1. General. The best deterrent against terrorism is alert, well trained personnel. To achieve the required level of training, a thorough program has been designed to ensure personnel are capable of protecting themselves and are capable or continuing to perform their duties while countering a terrorist threat.

2. Training

a. Level I Training

(1) Level I AT/FP training will be conducted for all military and civilian personnel should Threat Levels rise above Threat Level "LOW" within the continental United States (CONUS) or it's territories.

(2) Level I AT/FP training will be conducted by a level II qualified instructor within six months prior to OCONUS travel for deployment, permanent change of station (PCS), or temporary assigned duty (TAD). All AT/FP training will be documented in accordance with references.

b. Marine Corps Institute (MCI) course 02.10b, Terrorism Awareness for Marines, provides basic knowledge for combating terrorism for the individual Marine.

c. The following specialized training courses are available for Marines involved in physical or personnel security programs. Quotas and funding will be allocated by CMC (POS), CG MCCDC (T&E) or MARFORRES (G-3 Training).

(1) Course: Antiterrorism Instructor Qualification Course (2 weeks)
Location: U.S. Army, John F. Kennedy Special Warfare Center Ft Bragg, North Carolina
Scope: Designed to train already well-qualified instructors in antiterrorism measures. Students are required to prepare and deliver several blocks of instruction on such topics as terrorist history and organizations, awareness and avoidance, and hostage survival methods.

(2) Course: Terrorism Counteraction on Military Installations (1 week)
Location: US Army Military Police School, Ft Leonard Wood, Missouri
Scope: Designed for personnel serving in, or assigned to security staff positions supporting combating terrorism efforts. It teaches Marines proactive and reactive methods for developing a systematic approach to effectively counter the terrorist threat aboard bases and stations.

(3) Course: Individual Terrorism Awareness Course (1 week)
Location: US Army, John F. Kennedy Special Warfare Center Ft Bragg, North Carolina
Scope: Designed for personnel who are scheduled for overseas assignments to a moderate or higher threat area, to include deployments. It provides information on victim avoidance, and those counter-measures designed to reduce the risk of terrorist attack in a high threat environment. Course also teaches individual survival methods for Marines taken hostage by terrorists.

(4) Course: Dynamics of International Terrorism (1 week)
Location: Air Force Base, Hurlburt Field, Florida
Scope: Provides selected personnel with a basic understanding of the theory, psychology, organization, techniques and operational capability of terrorist groups on an international and regional basis.

(5) Course: High Risk Personnel (HRP) Course (5 days)
Location: Weapons Training Battalion, MCCDC, Quantico, Virginia
Scope: Designed to train personnel in special shooting techniques that may be required in a high-risk area. This course is restricted to personnel designated to fill overseas high-risk billets.

TRAVEL SECURITY POLICY

The worldwide presence of the Marine Corps increases its vulnerability to acts of terrorism. To establish consistency within DoD, the following standard guidance has been developed for use by all DoD components:

a. When official business requires travel to, or through, DoD-designated high or potential physical threat countries, DoD personnel and their dependents shall travel by military air or Air Mobility Command (AMC) charter whenever possible. The military services shall identify international airlift requirements to AMC. AMC is tasked to support those requirements with priority of support for travel to high physical threat countries. Theater commanders shall also identify intra-theater airlift requirements to AMC through their Air Force service components.

b. Members of the Uniformed Services and DoD civilian employees are authorized to use foreign flag airlines and/or indirect routings to avoid DoD-designated high or potential physical threat countries. Transportation officers who arrange travel through an indirect routing or on a foreign flag air carrier to avoid such areas should cite 57 Comp. Gen. 519 and 522 as the justification for using a foreign flag carrier. The use of that citation must be documented in each case and attached to each travel voucher. That citation is not authority to disregard totally the requirement in the Joint Federal Travel Regulations (JFTR), volume 1, paragraph U3125C; and the JFTR volume 2, paragraph C2204-2, to use U.S. air carriers where available. Travelers hereby authorized to avoid specific areas must disembark at the nearest interchange from point of origin and continue the journey on American flag carrier service.

c. Blanket approval and reimbursement for the use of regular fee passports is not authorized. The passport policy for DoD personnel and their family members traveling on official orders to and or from countries with no identified threat remains unchanged. DoD personnel shall travel on no fee official passports or on official orders with ID cards as required by the country visited. Command sponsored family members shall continue to use the no-fee regular passports with an official endorsement. DoD personnel and their families traveling on official orders to or from high or potential physical threat countries by commercial air are authorized, but not required, to obtain and

use the regular-fee passport for security reasons. Travelers electing to exercise that option are responsible for obtaining the regular fee passport and all required visas. Reimbursement for passports and visas obtained under those conditions is authorized by the JFTR, and payment shall be made on submission of appropriate documentation. Some countries have strict rules as to type of passport or visa required for entry. Information on the restrictions on the use of regular-fee passports can be obtained from local personnel offices before travel. Individuals traveling solely by military air or AMC charter shall not be reimbursed for regular-fee passports, unless U.S. Government transportation became available on short-notice (i.e., after commercial travel arrangements had been made and passport purchased), or priority of travel was sufficiently high to require backup travel arrangements. Payment for regular fee passports will not be reimbursed when said passports are used for personal travel.

d. Commercial airline tickets shall not be annotated to show any affiliation of the traveler to the U.S. Government.

e. Travel itineraries of high-risk personnel (to include general officers or civilian equivalents) will be marked "FOR OFFICIAL USE ONLY" at minimum when their travel takes them to, or through, designated high physical threat countries.

(3) Terrorism threat assessments, conducted annually or as required, shall be the basis and justification for recommendations on AT/FP enhancements, program/budget requests, and the establishment of specific unit (installation) THREATCON measures.

b. VAs will identify key assets and infrastructures located aboard and adjacent to the installation. VAs must address the impact of temporary or permanent loss of key assets or infrastructures to the unit's (installation's) ability to perform its mission. Commanders must identify those unit assets likely to become terrorist targets, paying particular attention to Mission Essential Vulnerable Areas (MEVAs) (see enclosures (6) through (8)).

c. At a minimum, assessments should address the functional areas of intelligence/counterintelligence, law enforcement (if applicable) and operations, physical security, civil, electrical and structural engineering, infrastructure, weapons effect mitigation, force protection plans and programs, and host nation support (for OCONUS installations) and local community support (for CONUS installations).

d. Pre-deployment AT/FP VAs must be conducted for all units prior to movement. These assessments will form the basis for unit AT/FP plans as well as appropriate force protection measures to reduce risk and vulnerability.

e. While the assessment of the terrorist threat is a command function, the Naval Criminal Investigative Service (NCIS) maintains a world-wide structure which provides criminal investigative and counterintelligence/antiterrorism support to Marine Corps commands, except those combat related counterintelligence matters within the functional responsibility of the Marine Corps. To fulfill this responsibility, NCIS has established the Navy Antiterrorism Alert Center (NAVATAC), which processes real time information and operates on a 24-hour basis. The NAVATAC provides the following support to Marine Corps commands:

(1) Navy Antiterrorist Alert Center Summary (ATACSUM)

(a) The ATACSUM is sent to all Marine Corps installations and major commands 6 days a week (excluding Saturdays).

TERRORIST THREAT AND VULNERABILITY ASSESSMENTS

1. General. All MARFORRES sites will, at a minimum, take the following measures to determine the terrorist threat to the site:

a. Conduct a quarterly terrorism threat brief. This brief may be conducted by a qualified AT/FP Officers. Units will obtain this brief annually from the appropriate NCIS Field Office Counterintelligence Agent listed in enclosure (1).

b. Annually obtain and review the installation threat assessment prepared by NCIS Anti Terrorism Alert Center (NCIS-ATAC)

c. Make and maintain liaison with the base security officer or local law enforcement agencies regarding local terrorist threats.

2. Vulnerability Assessments

a. Vulnerability Assessments (VAs) will be conducted at least annually. VAs will focus on those elements directly relating to combating terrorism, including mitigation, preparedness, facilities, response and recovery. Assessments identify vulnerabilities that may be exploited by threat groups and recommend options to reduce or eliminate those vulnerabilities. Two methods of vulnerability assessment will be used.

(1) Local Assessment. Qualified unit AT/FP Officers will conduct a VA of the site annually in accordance with this order and references (a) through (d). This assessment will be forwarded to MARFORRES, A/CS G-3 (ATTN: AT/FP Officer).

(2) Outside Agency Assessment. Units located at sites owned or leased by Marine Forces Reserve will request a VA be conducted by an outside agency once every three years. This assessment may be conducted in conjunction with the Commanding Generals Inspection (CGI) if vulnerability assessment teams are available. VAs will be requested through the MARFORRES AT/FP Officer. Joint Task Force-34 (J-34), MARFORRES Counter-intelligence Teams (CIT) and the MARFORRES AT/FP Office are trained to conduct VAs.

(b) It provides current operational intelligence on terrorist and related unconventional warfare threats to Department of the Navy (DON) personnel and assets, to include establishing the threat levels for specific geographic areas.

(2) NAVATAC Force Protection Summary. The Force Protection Summary is published weekly and lists countries designated by DoD as Medium to Critical terrorist threat levels. Additionally, when changes to country threat levels occur they are published in the Summary.

(3) NAVATAC Warning Report

(a) The NAVATAC Warning Report is sent to affected commands only.

(b) It provides threat specific information on impending or likely terrorist activity, to include establishing, the threat levels for specific geographic areas.

(4) NAVATAC Spot Report

(a) The NAVATAC Spot Report is sent to affected commands only.

(b) Reports provide indications and warnings of imminent terrorist activity and advise of activities, conditions, or events which could lead to near-term terrorist operations directed against DON assets or personnel.

(5) NAVATAC Threat Assessment

(a) An assessment is made for commanders upon request of:

1 Marine Corps installations

2 Major tenant commands aboard Marine Corps installations (Marine Divisions, Marine Aircraft Wings, Force Service Support Groups, etc.).

3 Marine Corps units deploying outside of the continental United States. (Deployed units embarked aboard Navy ships in the Mediterranean Sea will automatically receive a

threat assessment at least 7 to 10 days prior to commencement of each port call).

4 Marine Corps units that are not tenants aboard a Marine Corps installation (Reserve units, Marine Corps districts, etc.).

(b) This threat assessment provides current operational intelligence on terrorist and related unconventional warfare threats, for the geographic area specified, to include the establishment of a threat level for that specific area.

(c) Requests to receive this assessment should be submitted in writing through the supporting Naval Criminal Investigative Service Resident Agency (NCISRA) at least 2 weeks prior to the date the assessment is required.

(6) NAVATAC Threat Briefing

(a) This briefing is provided to requesting commands preparing for deployment outside CONUS.

(b) It is conducted by a NAVATAC representative.

(c) It provides unit personnel with an overview of the general terrorist threat and specifics on the threat in the geographic area where the unit will deploy.

(d) Requests for this briefing should be submitted in writing through the supporting NCISRA at least 1 month prior to the scheduled briefing date. Requesting commands must fund travel and per diem for briefing personnel.

f. NAVATAC THREAT LEVEL CONSIDERATIONS. The following factors are considered by NAVATAC prior to establishing a threat level:

(1) Existence. A terrorist group is present, assessed to be present, or able to gain access to a given country or locale.

(2) Capability. The acquired, assessed, or demonstrated level of ability to conduct terrorist attacks.

(3) Intentions. Recent demonstrated anti-U.S. terrorist activity, or stated or assessed intent to conduct such activity.

(4) History. Demonstrated terrorist activity over time.

(5) Targeting. Current credible information on activity indicative of preparations for specific terrorist operations

(6) Security environment. The internal policy and security considerations that impact on the capability of terrorist elements to implement their intentions.

g. NAVATAC THREAT LEVELS. To establish a threat level, the NAVATAC assesses which of the following five threat levels describe the likelihood of the threat:

(1) Critical. Factors of existence, capability, and targeting must be present. History and intentions may or may not be present.

(2) High. Factors of existence, capability, history, and intentions must be present.

(3) Medium. Factors of existence, capability, and history must be present. Intentions may or may not be present.

(4) Low. Existence and capability must be present. History may or may not be present.

(5) Negligible. Existence and/or capability may or may not be present.

h. Although threat assessments performed by NAVATAC will normally provide the commander with sufficient information to make prudent security determinations, such assessments must not be considered "stand alone" documents. Commanders must ensure threat assessments are kept up to date. The local NCISRA can provide current antiterrorism information necessary to continually assess the terrorist threat.

TERRORIST THREAT CONDITIONS (THREATCON's)

1. THREATCON. The decision to arrive at a particular THREATCON and associated security measures should be based on multiple factors, which may include, but are not limited to:

a. The threat

b. Target vulnerability

c. Criticality of assets

d. Security resources availability

e. Operational and moral impact of security measures

f. Damage control and recovery procedures

g. International relations

h. Planned U. S. Government actions, which could trigger a terrorist response

2. THREATCON MEASURES. THREATCON measures should be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise.

3. THREATCON MODIFICATION

a. Units and organizations located in civilian communities (recruiting stations, Marine Corps Reserve units, etc.) should modify THREATCON measures at each level to meet their own unique requirements and based on the assessment of local threat conditions.

b. Units that are tenants will follow the THREATCON of the host station or organization.

4. THREATCON NORMAL. A general threat of possible terrorist activity exists, but warrants only a routine security posture.

5. THREATCON ALPHA. A general threat of possible terrorist activity against personnel and installations exists, the nature

and extent of which are unpredictable. Circumstances do not justify full implementation of THREATCON BRAVO measures; however, it may be necessary to implement certain selected measures from higher THREATCONS. This decision may be based on intelligence received, or the need to provide a specific deterrent. The measures in THREATCON ALPHA should be sustainable for an indefinite period.

a. Measure 1. Remind all personnel, including family members, at regular intervals to:

(1) Be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers.

(2) Be alert for unidentified vehicles on, or in the vicinity of U.S. installations, units, or facilities.

(3) Be alert for abandoned parcels, suitcases or any unusual activity.

USMC recommended, Measure 1-1: Troop information program: Brief all personnel on the current threat condition, and those measures enacted to increase security. Remind all duty personnel to be especially alert for suspicious or unusual activity, strangers, or unidentified vehicles.

USMC recommended, Measure 1-2: Conduct unit level terrorism awareness training.

b. Measure 2. Keep the Duty Officer or other appointed personnel having access to plans for evaluating or sealing off buildings and/or areas in use, or where an explosion or attack has occurred, available at all times. Keep key personnel who may be needed to implement security plans on call.

USMC recommended, Measure 2-1: Ensure duty personnel have knowledge of, and access to emergency plans. (Give special attention to the evaluation of buildings and grounds in use, as well as the plans for cordoning off areas.)

USMC recommended, Measure 2-2: Establish on call duty roster of heavy equipment operators. All off-duty heavy equipment operators will report their destination and expected time of return to the military police desk (or the duty officer/NCO for

units without a provost marshal) prior to leaving their listed recall address.

c. Measure 3. Secure buildings, rooms, and storage areas not in regular use.

d. Measure 4. Increase security spot checks of vehicles and persons entering installations and nonclassified areas under the jurisdiction of the U.S. command or agency.

USMC recommended, Measure 4-1: Installation military police (MP) institute random identification spot checks of passenger and commercial vehicle occupants entering the base or installation, using predetermined criteria for vehicle selection. if possible, delays in traffic beyond 8 to 10 minutes should be avoided.

USMC recommended, Measure 4-2: Installation MP, with or without the assistance of military working dog (MWD) teams, conduct daily Commanding Officer's administrative vehicle inspections at random times and locations.

USMC recommended, Measure 4-3: Installation MP physically inspect and verify license plates affixed to vehicles entering the base or installation.

USMC recommended, Measure 4-4: Installation MP check the identification card, drivers license and/or vehicle registration card of all passenger vehicle and commercial truck drivers, and the identification card of vehicle occupants and pedestrians (to include joggers and bicyclists).

e. Measure 5. Limit installations access points for vehicles and personnel, commensurate with a reasonable traffic flow.

f. Measure 6. As a deterrent, apply one of the following measures from THREATCON BRAVO individually and randomly:

(1) Secure and regularly inspect buildings and storage areas not in regular use.

(2) At the beginning and end of each workday and at frequent intervals, inspect the interior of buildings in regular use for suspicious packages or activity.

(3) Check all deliveries to messes, clubs, etc. (Advise family members to check all home deliveries.)

(4) As far as resources allow, increase surveillance of domestic accommodations, schools, messes, clubs, and other "soft targets" to improve deterrence and defense, and to build confidence among staff and family members.

g. Measure 7. Review all plans, orders, personnel details, and logistic requirements related to the introduction of a higher THREATCON.

USMC recommended, Measure 7-1: Convene the Installation Security Council to review incident response plans.

h. Measure 8. As appropriate, review and implement security measures for high-risk personnel; e.g., direct the use of inconspicuous body armor.

i. Measure 9. As appropriate, consult local authorities on the threat, and mutual AT measures.

USMC recommended, Measure 9-1: The installation PMO will notify adjacent police jurisdictions of threat conditions in effect at the base or installation, and continue to exchange intelligence.

USMC recommended, Measure 9-2: The commander and key staff review installation contingency plans.

USMC recommended, Measure 9-3: Jurisdiction and command and control issues are agreed upon and exercised between FBI and local or host-nation agencies.

j. Measure 10. Spare.

USMC recommended, Measure 10-1: Place barriers in "ready" position near gates and/or sensitive buildings, where they may be required to provide blocking, delaying or channeling actions.

USMC recommended, Measure 10-2: Establish countersurveillance in areas likely to be targeted by hostile elements.

6. THREATCON BRAVO. This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this THREATCON must be capable of being maintained

for weeks without causing undue hardship, affecting operational capability, or aggravating relations with local authorities.

a. Measure 11. Repeat measure 1 in paragraph 4a above, and warn personnel of any other terrorist form of attack.

USMC recommended, Measure 11-1: Unit security managers continue the threat briefing/information/orientation process for all personnel, with particular emphasis toward reporting suspicious incidents and persons.

b. Measure 12. Keep all personnel involved in implementing antiterrorist contingency plans on call.

USMC recommended, Measure 12-1: Key staff members continue preparation for implementing AT Contingency plans.

USMC recommended, Measure 12-2: All members of the crisis management team (CMT), off-duty military police, primary reaction platoon personnel, and other members of the crisis management force (CMF) report their destination and expected time of return to the MP desk sergeant or other designated official prior to leaving their listed recall address.

USMC recommended, Measure 12-3: As far as resources allow, assign a driver and/or MP trained in protective service operations to the base commander, general officers, or other designated personnel with significant terrorist target value.

USMC recommended, Measure 12-4: The provost marshal directs a periodic recall of the special reaction team (SRT), if one is established.

c. Measure 13. Check plans for implementation of the measures in the next higher THREATCON.

d. Measure 14. Where possible, move cars and objects such as crates, trash containers, etc., at least 25 meters from buildings, particularly those buildings of a sensitive or prestigious nature. Consider the application of centralized parking.

e. Measure 15. Secure and regularly inspect all buildings, rooms, and storage areas not in use.

f. Measure 16. At the beginning and end of each workday and at other regular and frequent intervals inspect the interior and exterior of buildings in regular use for the presence of suspicious objects and packages.

USMC recommended, Measure 16-1: Security and law enforcement (if applicable) personnel increase physical security checks of facilities after normal working hours.

USMC recommended, Measure 16-2: Explosive Detector MWD teams check the exterior of vehicles in the parking lots immediately adjacent to headquarters and other sensitive buildings.

g. Measure 17. Examine all incoming mail for letter or parcel bomb devices.

h. Measure 18. Check all deliveries to messes, clubs, etc.

USMC recommended, Measure 18-1: Designated personnel and employees randomly check package deliveries brought into service areas.

USMC recommended, Measure 18-2: Military dependents are advised to check all home deliveries, and to report all suspicious letters and packages.

USMC recommended, Measure 18-3: Military police search all commercial vehicles entering the installation, and compare vehicle contents with bills of lading or other manifest documents.

i. Measure 19. As far as resources allow, increase surveillance of domestic accommodations, schools, messes, clubs, and other "soft targets."

USMC recommended, Measure 19-1: Military police MWD teams conduct walking patrols of selected parts of the installation's housing area perimeter fenceline.

USMC recommended, Measure 19-2: The installation commander implements regulations prohibiting the carrying of parcels into exchanges, clubs, and other designated buildings, except for specific circumstances and through specific doors where they will

be checked for contraband. Signs indicating the new regulations should be conspicuously posted at these selected sites.

USMC recommended, Measure 19-3: Security and law enforcement (if applicable) personnel increase patrolling of "soft targets" such as bachelor enlisted quarters (BEQ) and exchanges.

j. Measure 20. Make organizational staff and dependents aware of the general situation in order to stop rumors and prevent unnecessary alarm.

k. Measure 21. At an early stage, inform members of local security committees of any action being taken and why.

l. Measure 22. Physically inspect visitors to the unit, and a percentage of their suitcases, parcels, and other containers.

USMC recommended, Measure 22-1: Commanding Officers reduce authorized access points of all buildings under their cognizance, direct random ID checks at all building entrances, and direct the physical inspection of handbags, briefcases and parcels of all visitors.

USMC recommended Measure 22-2: Commanding Officers direct 100 percent identification card checks at buildings which are, or contain, high value targets.

USMC recommended, Measure 22-3: Security personnel physically inspect all guests ("official visitors" may be exempted), and escort all visitors.

USMC recommended, Measure 22-4: While issuing visitor passes, MP conduct a physical inspection of visitors entering the installation, to include their suitcases, parcels and other containers.

m. Measure 23. Whenever possible, operate random patrols to check vehicles, people, and buildings.

USMC recommended, Measure 23-1: Installation MP mobile patrols check roads adjacent to the installation's perimeter fenceline, and report suspicious off-base circumstances to the servicing law enforcement (if applicable) agency. Installation perimeter fencelines not accessible by vehicles should be checked on foot or by MWD teams.

n. Measure 24. Protect off-base military personnel and military transport in accordance with prepared plans. Remind drivers to lock parked vehicles, and to institute a positive system of checks before entering and driving their vehicle.

o. Measure 25. Implement additional security measures for high-risk personnel, as appropriate.

USMC recommended, Measure 25-1: Use frost calls and base/station cable television to disseminate information and directions such as the use of civilian attire, off-limits lists, alternate reporting times, etc.

USMC recommended, Measure 25-2: Train unit high-risk personnel in incident response and emergency aid procedures.

p. Measure 26. Brief personnel, who may augment guard force, on the use of deadly force and the rules of engagement.

q. Measure 27. As appropriate, consult local authorities on the threat and mutual AT measures.

USMC recommended, Measure 27-1: Emplace barriers at gates near sensitive building, and per the installation's barrier plan.

USMC recommended, Measure 27-2: Support emplaced barriers with sufficient observation.

r. Measures 28 and 29. Spare.

7. THREATCON CHARLIE. This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and installations are imminent. Implementation of this measure for more than a short period will probably create hardship, and affect the peacetime activities of the unit and its personnel.

a. Measure 30. Continue all THREATCON BRAVO measures, or introduce those measures still outstanding.

b. Measure 31. Keep all personnel responsible for implementing antiterrorist plans available at their place of duty.

c. Measure 32. Limit access points to the absolute minimum.

d. Measure 33. Strictly enforce entry control, and search a percentage of vehicles.

e. Measure 34. Enforce centralized parking of vehicles away from sensitive buildings.

f. Measure 35. Issue weapons to guards (local orders should include specific orders on the issue of ammunition).

Note: Marine Corps regulations already prescribe the issuance of loaded weapons to all personnel engaged in law enforcement (if applicable) or security duties.

g. Measure 36. Introduce increased patrolling of the installation.

h. Measure 37. Protect all designated mission essential vulnerable areas (MEVAS) and vulnerable points (VPs). Give special attention to MEVAs and VPs outside of military establishments.

i. Measure 38. Erect barriers and obstacles to control traffic flow.

j. Measure 39. Consult local authorities about closing public (and military) roads or facilities that make the site more vulnerable to terrorist attacks.

k. Measure 40. Spare.

8. THREATCON DELTA. Implemented in the immediate area where a terrorist attack has occurred, or when intelligence has been received that terrorist action against a specific location is likely. Normally, that THREATCON is declared as a localized warning.

a. Measure 41. Continue or introduce all measures listed for THREATCON BRAVO and CHARLIE.

b. Measure 42. Augment guards, as necessary.

c. Measure 43. Identify all vehicles already on the installation within operations or mission support areas.

d. Measure 44. Search all vehicles entering the

installation, as well as their contents.

e. Measure 45. Control all access, and implement positive identification of all personnel.

f. Measure 46. Search all suitcases, briefcases, packages, etc., brought into the complex or installation.

g. Measure 47. Take measures to control access to all areas under the jurisdiction of the US command or agency concerned.

h. Measure 48. Make frequent checks of the exteriors of buildings and parking areas.

i. Measure 49. Minimize all administrative journeys and visits.

j. Measure 50. Coordinate the possible closing of public and military roads and facilities with local authorities.

k. Measure 51. Spare.

8. REPORTING CHANGES IN THREAT CONDITION (THREATCON). Units will report any change in THREATCON status to the appropriate Major Subordinate Command (MSC) with an information copy to the MARFORRES A/CS G-3 (ATTN: AT/FP Officer).

INDIVIDUAL PROTECTIVE MEASURES

1. Keep a low profile. Your dress, conduct, and mannerisms should not attract attention. Make an effort to blend into the local environment. Avoid publicity and don't go out in large groups. Stay away from civil disturbances and demonstrations.

2. Be unpredictable. Vary your route to and from work and the time you leave and return home. Vary the way you dress. Don't exercise at the same time and place each day, never alone, on deserted streets, or country roads. Let people close to you know where you're going, what you'll be doing, and when you should be back.

3. Be alert. Watch for anything suspicious or out of place. Don't give personal information over the telephone. If you think you are being followed, go to a preselected secure area. Immediately report the incident to the military/security police or law enforcement agencies. In overseas areas without such agencies, report the incident to the Security Officer or the military attaché at the US Embassy.

4. Plan ahead. As a member of the US Marine Corps, you are a potential hostage. When in a high terrorist risk area, one of the first things to do is prepare for your own personal contingencies. You can prepare for the rigors of captivity, which will offer some peace of mind in the event you are held captive.

a. Maintain family and personal affairs in good order. REDs, wills, powers of attorney, and financial plans should be current.

b. Discuss with your family what to do in event of your abduction. Prepare a package of instructions, money, airline tickets, credit cards, insurance policies, and whom to contact for survivor assistance.

c. Have a supply of essential medicines and first aid items. If necessary, ask for more and accept what is provided.

d. Do not travel with documents on your person. You can be asked to explain names, phone numbers, addresses, etc. If held captive, try to convince your captors they have taken the wrong

individual.

5. Actions if Attacked

a. Dive for cover. Do not run. Running increases the probability of shrapnel hitting vital organs, or the head.

b. If you must move, belly crawl or roll. Stay low to the ground, using available cover.

c. If you see grenades, lay flat on the floor, feet and knees tightly together with soles toward the grenade. In this position, your shoes, feet, and legs protect the rest of your body. Shrapnel will rise in a cone from the point of detonation, passing over your body.

d. Place arms and elbows next to your ribcage to protect your lungs, heart, and chest. Cover your ears and head with your hands to protect neck, arteries, ears, and skull.

e. Responding security personnel will not be able to distinguish you from attackers. Do not attempt to assist them in any way. Lay flat and don't move until told to get up.

PHYSICAL SECURITY PLAN

1. General. Physical security protects and safeguards personnel from criminal and terrorist acts. A physical security program should be designed to deny access, delay intruders and detect unauthorized access. The Commanding Officer is responsible for all physical security within the command and the external security of all facilities within the confines of any Naval Installation.

2. Physical Security Plan. A Physical security plan will outline the security measures (active and passive) used to prevent unathorized access to personnel, equipment, installation, material and documents. Physical security plans will be tailored according to the local threat and security requirements as determined by the installation/unit commander. An example physical security plan is located at the end of this enclosure.

3. Duties

a. Unit Security Officer. Under the direction of the Commanding Officer, the Security Officer is responsible for the establishment, administration, and coordination of physical security and law enforcement (if applicable) involving the protection of Naval and specified governmental agencies at the unit activity, military personnel, employees, and dependents. The Security Officer:

(1) Provides advisory assistance to the Commanding Officer for overall installation security, law enforcement (if applicable), and the maintenance of good order and discipline.

(2) Establishes and maintains effective liaison with the Naval Criminal Investigative Service Resident Agency (NCISRA), the local Police Department, State Police, and national law enforcement (if applicable) agencies, in connection with criminal investigations, police matters, and security of military installations.

(3) Coordinates physical security requirements with personnel of the command.

(a) Protects installation assets and personnel against sabotage, espionage, theft of Government property, and

any covert act that may be detrimental to the unit mission.

(b) Identifies and makes recommendations concerning the designation of security areas and measures to protect areas such as industrial complexes and populated areas including:

1 Monitoring of mechanical, electrical, and electronic security devices and sensors.

2 Providing military police and guard services commensurate with manpower and budgetary constraints.

3 Protecting the integrity of the installation by conducting perimeter security patrols.

(c) Exercises local operational control over:

1 Military and civilian law enforcement (if applicable) personnel.

2 Investigators.

(d) Controls all personnel, material, and vehicles entering or exiting the installation by:

1 Administering a pass and identification system.

2 Establishing and enforcing a base traffic code that delineates the procedures for vehicle registration, vehicle and traffic regulations, and traffic law enforcement (if applicable), accident investigation, and Naval Traffic Court.

3 Conducting random inspection of personnel and vehicles entering or exiting the installation to prevent illegal admission of drugs, contraband, or dangerous weapons; to prevent the removal of Government and personal property; and to prevent the exit of contraband and illicit goods into the local community. Inspections will also be conducted prior to major unit deployments OCONUS.

(e) Supervises law enforcement (if applicable) and the maintenance of good order and discipline by:

1 Enforcing all local and U.S. Navy regulations

and directives related to physical security and law enforcement (if applicable) affecting the installation and its population.

2 Responding to all violations of the Uniform Code of Military Justice (UCMJ) or US Navy directives by military personnel, and apprehending and effecting initial disposition of offenders.

3 Apprehending and effecting the initial disposition of stragglers, absentees, deserters, and prisoners in coordination with the Staff Judge Advocate (SJA).

4 Reporting all violations of the UCMJ, Navy directives, or base regulations to the offender's Commanding Officer.

5 Enforcing pet regulations and animal control measures.

6 Accomplishing various other related tasks as necessary or directed by the Commanding Officer.

b. Commanders of Tenant Units. The commander of a unit that is a tenant of an installation or base will:

(1) Coordinate their internal security with the Senior Installation Security Officer.

(2) Designate an officer as the Physical Security Officer. Physical Security Officers shall have cognizance over all internal physical security for their command and will coordinate their requirements for additional support with the Senior Installation Physical Security Officer or with MARFORRES. The Physical Security Officer has traditionally been appointed from the Intelligence or Military Police sections.

(3) Develop and maintain a physical security plan for their activity complying with the guidelines of reference (a) and (c) and this instruction. The plan will be submitted to the MARFORRES Security Officer for review and recommendations.

(4) Commanding Officers who have security forces available for internal security will approve and sign the guard orders for the guard posts within their area of responsibility.

(5) Ensure that personnel standing watches are trained and equipped; and those copies of watch assignments are forwarded to the Installation Security Officer (if applicable).

(6) Ensure timely reporting of all incidents to the Installation Security Officer or designated representatives.

4. Physical Security Education and Training. The Security Officer will develop and coordinate a command Physical Security Training Program. The training program will include:

a. Physical Security Standards and Procedures

b. Loss Prevention

c. Identification and Reporting of Security Violations

d. Improvement of Security Measures

e. Antiterrorism Training and Pre-deployment Briefs

5. Waivers and Exceptions. Any variance with required security criteria, temporary or permanent, will have a waiver or exception approved by higher authority. Waiver/exception requests will be submitted per references (a) and (c).

6. Priorities. MARFORRES Physical Security Program/resource priorities shall be based on the most current threat analysis and vulnerability information. These priorities will determine the urgency for completion of security projects, upgrades, etc. Security priority levels:

a. Protection of mission assets.

b. Protection of life/safety assets (Commissary, quarters, offices, etc.).

c. Protection of valuable assets (Navy Exchange, Morale, Welfare and Recreation (MWR) properties, etc.).

7. Threat Analysis. NCISRA will provide a threat assessment profile for Reserve commands. This report, unless classified, will be included as an Annex to the Physical Security Plan. Classified reports will be kept under separate cover.

8. Vulnerability. The NCISRA threat analysis report and periodic Physical Security Surveys, along with other security inspection reports and security violation data, will be used to determine the overall current vulnerability of command installations, and will be used to assist in establishing Physical Security Program priorities.

9. Physical Security Surveys. Physical Security Surveys will be conducted at least annually by all departments/commands. Results of these surveys will be documented and kept on file for two years.

a. The Command Security Officer will perform periodic surveys of all command facilities. Such surveys, when they cover an entire department/command, may be counted as completion of the annual survey requirement.

b. A copy of the results of each department's/command's physical security survey will be supplied to the MARFORRES Security Officer for review/coordination.

c. Tenants may request, in writing, assistance from the MARFORRES Security Officer, Physical Security Officer or Antiterrorism Officer, however, he/she will not routinely perform physical security surveys for tenant activities.

d. Reports generated by Physical Security Surveys may be used to upgrade local security measures/programs. They will not be forwarded to higher authority via MARFORRES. Use of these reports by tenant commands is subject to requirements of the respective commands.

(1) Reports submitted by commanders will be subject to review by the Force Protection Officer to coordinate Reserve-wide security measures, upgrades, etc.

(2) Department heads will use these reports to document and monitor corrections of security deficiencies within their respective areas and to identify those areas requiring waivers or exceptions.

10. Physical Security Terms and Definitions

a. Protective Barriers and Security Aids. Physical

barriers, signs, and devices are designed to restrict, impede access, or announce the presence of an intruder. Physical perimeter barriers at unit locations can be both natural and structural. Security aids range from a simple lock, to intrusion detection system, to manpower resources to combat and deter criminal elements, saboteurs, and espionage.

(1) Perimeter Protective Fencing. When possible, all land boundaries of unit locations should be fenced and the specifications will meet the requirements of reference (a). The fence line will be routinely inspected by commanders to ensure all damages and discrepancies are corrected immediately. This fencing is contingent on property lease agreements and availability of funding by this headquarters Facilities Department.

(2) Perimeter Clear Zones. Clear zones will be maintained on both the inside and outside of the perimeter fence line as required by reference (a) or as waived or excepted by higher authority. Routine clearing and/or mowing will be conducted to ensure zones and fence lines are kept clear.

(3) Perimeter Water Boundary. A body of water used as a perimeter boundary will be routinely patrolled to prevent unauthorized entry by boaters or swimmers.

b. Manning of Perimeter Gates, Points of Entry/Exit. Trained, armed Security Force personnel will man all land boundary gates when open. All gates not manned will be secured with a medium security padlock and the key controlled by the Security Department. The department or activity having cognizance over such areas during normal operating hours will man all authorized water access points. Signs will be conspicuously posted on piers and landings, warning all persons that entry is only authorized as follows:

(1) Prearrangement and authorization by Commanding Officer of the unit or installation.

(2) Near water boundaries an emergency berthing of craft due to water or weather conditions, serious property damage, or life threatening conditions is a reality in different cases. In these cases, the Security Officer and Command Duty Officer (CDO/OOD) will be contacted immediately.

c. Perimeter Locks. Only approved perimeter locks will be used. Lock standards and Lock Control Procedures are located in reference (d).

d. Physical Security Electronic Equipment (PSEE). PSEE is designed to detect actual or attempted entry or penetration. Resources requiring continuous or frequent security checks due to essential or critical classification, will be studied for the feasibility of PSEE protection.

e. Activated Intrusion Detection Systems (IDS). When a signal is received at the security office indicating an alarm or trouble on the line, the police dispatcher will immediately dispatch a sufficient number of police officers to secure the affected area. Standard operating procedures for each alarmed area will be established and practice exercises will be conducted quarterly. The following will be accomplished on each IDS circuit:

(1) Each alarm activation, real, false, or trouble, will be recorded in an IDS alarm log at the Security Department. Each entry will show the time, date, location, cause of alarm, and action taken.

(2) Each activity or department with IDS will provide an up-to-date IDS recall roster to the security or police division.

(3) Personnel on the recall roster will respond immediately when notified.

(4) The security or police officer on the scene will use caution and accepted practices in securing the area and determining if an intrusion has actually occurred.

(5) Tenants using PSEE will include local procedures, standards, and policies for effective use and maintenance. If connected to installation systems, tenants must ensure compliance with installation guidelines.

f. Security Lighting. Security lighting will be provided as required and will meet specification standards per reference (a) for all restricted areas. Security lighting for all other areas will be sufficient to provide a deterrent against theft, vandalism, and criminal activity. Lighting requirements and placement will be coordinated by the Security Officer and the

Public Works Officer. Defective and burned out security lights will be repaired/replaced immediately.

g. Security Force Communications. Installations that maintain a Security Police/Guard Force will have its own communications, with direct lines between security headquarters and security elements, and an auxiliary power supply and sufficient equipment to maintain continuous two-way voice communications among each element.

(1) Purpose. Security communications will provide the following:

(a) Expeditious transmission of routine and emergency instructions between security headquarters, posts, and patrols.

(b) Integration and coordination of security functions.

(c) Efficient and economical use of security forces.

(d) Expeditious transmission of requests for assistance to outside sources in an emergency beyond Security's capability to control.

(e) The use of the "10" code with other suitable and uniform radio voice communications system.

(2) Security Communications Equipment. Security communications include all telephone systems (field, local, government, and commercial) and all radio systems (portable, mobile, or fixed) which can be used for rapid and reliable two-way voice communications.

(3) Use of Security Communications Systems is limited to official use only by the Security Department, the Commanding Officer, the Executive Officer and the CDO/OOD.

(4) Testing of Security Communications Systems

(a) Fixed base, mobile and portable stations will be tested at the beginning of each shift. Discrepancies will be recorded and reported.

(b) Tests will be conducted quarterly under simulated

emergency conditions. A record/log of all testing, results and action taken to correct discrepancies will be maintained for a period of two years or until the next Inspector General or command inspection, whichever occurs first.

(5) Authentication of Communications. Duress codes will be assigned on a monthly basis to alert all security personnel of emergency situations. This code will be changed immediately if compromised.

h. Restricted Areas. All unit/installation areas should afford protection. Critical and essential areas should have higher degrees of protection and security control. Each commanding officer is responsible and has the authority to establish various levels of security protection for their areas. Tenant commands and activities may request assistance from the Installation Security officer in establishing restricted areas. These are areas that require control of access, and are classified into three types by the following criteria:

(1) Exclusion Area. An exclusion area is one containing classified matter of such nature that access to the area constitutes access to such classified information. The following basic security measures are required for an exclusion area:

(a) A clearly defined perimeter barriers.

(b) A personnel identification and control system.

(c) All points of ingress and egress are guarded or secured and alarm protected.

(d) Only persons whose duties actually require access and who have been-granted appropriate security clearances shall be allowed into exclusion areas.

(2) Limited Area. A limited area is defined as one containing classified matter in which uncontrolled movement would permit access to such matter; but within which escort and other internal restrictions and controls may prevent such access. The following basic security measures are required for all limited areas:

(a) A clearly defined perimeter barrier.

(b) A personnel identification and control system.

(c) All points of ingress and egress must be guarded or controlled by persons whose duties include identification checks, or they shall be monitored by automated surveillance systems.

(d) All persons admitted to a limited area with freedom of movement within such area shall have appropriate security clearances. Persons who have not been cleared for access to the information contained within a limited area may, with appropriate approval, be admitted to such area. Escort shall control them and security procedures to prevent access to the classified information.

(3) Controlled Area. A controlled area is defined as one adjacent to or encompassing limited or exclusion areas and within which uncontrolled movement does not permit access to classified matter. It is designed for the principal purpose of providing administrative control, safety, and/or a buffer area of security restrictions for limited or exclusion areas. The following basic security measures are required for a controlled area:

(a) A clearly defined perimeter.

(b) A personnel identification and control system.

(c) Identification checking installation at all regularly used points of access.

(d) Security and administrative arrangements for determining the need for access and method of approval for access to the area. Under normal conditions, approval for access to a controlled area will be based on operational need for access and adequate identification of the individual rather than on their security clearance status.

i. Security Violations. Any breach of security or violation of security control measures in any unit/installation restricted area should be reported to the command's Security Officer for action. Tenants may request assistance or advice concerning violations within their areas.

(1) Persons improperly entering restricted areas are subject to apprehension by installation police and disciplinary

action.

(2) Persons operating vehicles in restricted areas without authorization are subject to disciplinary action, including loss of driving privileges.

(3) Vehicles parked within restricted areas without approval of the Security Officer may be impounded by installation police on orders of the Commanding Officer. Such vehicles will be released to owners only as authorized by the Commanding Officer.

j. Hostage Situations. Due to the close proximity of law enforcement agencies in the continental U.S., and the extensive training required to successfully conclude a hostage situation, responses will be limited to:

(1) Take no direct action against the hostage taker(s)

(2) Notify base/station security personnel or local law enforcement agencies immediately. Provide the following information if available:

(a) Location and physical description of barricade.

(b) Number and identity of hostage takers.

(c) Any known reasons for taking hostages.

(d) If hostage takers are armed/types of weapons.

(e) Number and identity of hostages.

(f) Number of police personnel on-the-scene.

(g) Safest approach route.

(3) Do not fire on or return the fire of a hostage taker except in self-defense against certain death/grievous bodily injury.

(4) Retire to safe position in view of the area.

(5) Effect containment to the smallest possible area.

(6) Commence notification and recall of key personnel.

k. Proprietary Jurisdiction. The Federal Government has acquired a degree of ownership of a piece of property but has not obtained legislative authority over the area. Generally, only the state has the power to enforce its laws on the property. The Federal Government has the right, however, as does any landowner or tenant, to protect its property and personnel. In addition, state authorities cannot interfere with any valid military activity on such property.

PHYSICAL SECURITY PLAN FORMAT

CLASSIFICATION

Copy no. ____ of ____ copies
Issuing Headquarters
Location
Date/time group

1. PURPOSE. (State plan's purpose.)

2. AREA SECURITY. (Define the areas, buildings and structures considered critical. Establish priorities for their protection.)

3. CONTROL MEASURES. (Define and establish restrictions on access to and movement into critical areas.)

a. Personnel Access. (Establish control pertinent to each area or structure. Determine access authority. Provide access criteria for unit personnel, visitors, maintenance or support personnel, contractor personnel and local police/armed forces. Describe the system used in each area. If a badge system is used, provide complete descriptions to disseminate requirements for identification and control of personnel. Identify application of of control system for unit personnel, visitors to restricted or administrative areas, vendors, tradesmen, contractor personnel and maintenance or support. personnel.)

b. Material Control. (State incoming and outgoing material control requirements. Identify material admission requirements, inspection procedures, special controls on delivery of supplies and/or personnel shipments in restricted areas, and required documentation.)

c. Vehicle Control. (Identify vehicle registration policy, search policies, parking regulations and controls for entering restricted and administrative areas. Procedures must address privately owened, military and emergency vehicles.)

4. AIDS TO SECURITY. (Identify the installation's security procedures for protective barriers, protective lighting systems, intrusion detection systems and communications. Define the protective barrier's clear zones, signs (type and posting requirements) and gates (hours of operation, security

ENCLOSURE (15)

requirements and lock security). State the protective lighting system's use and control, inspections, response to commercial power failure, response to alternate source of power failure and emergency lighting system. State the intrusion detection system's security classification, inspection procedures, use and monitoring, response to alarm conditions, maintenance requirements, alarm logs or registers, sensitivity settings, fail-safe and tamper-proof provisions and monitor panel location. State communication locations, use, test and authentication procedures.)

5. INTERIOR GUARD PROCEDURES. (Include general instructions for interior guard personne. Detailed instructions are attached as annexes. Incorporate randomness in patrol procedures. Address composition and organization for security and alert force for: tour of duty, essential posts and routes, weapons and equipment, training, use of WMD teams, method of challenging, and ROE and deployment concept.)

6. CONTINGENCY PLANS. (Identify emergency response. Attached detailed plans (e.g., counterterrorism, bomb threat, diaster, fire) as annexes. Address individual actions, alert force actions and security alert status.)

7. SECURITY ALERT STATUS. (Determine current security alert status.)

8. USE OF AIR SURVEILLANCE. (State if air surveillance is/is not to be exploited and describe use and communications means.)

9. COORDINATING INSTRUCTIONS. (Identify integration plans of nearby military installations. State liaison and coordination instructions for local authorities, federal agencies and other military organizations.)